

WHAT IS CLAIMED IS:

1. A method for maintaining synchronization between a key used by a first node to encrypt information within information blocks that are transmitted via a communications network to a second node and a key used by said second node to decrypt information within information blocks received from said first node, each information block including a header and a payload, said method comprising:
 - distributing a new key between a first node and a second node; and
 - signaling, to one of said first and second nodes, a switch to said new key with a switch-to-new-key code that is not part of said header or said payload of any of said information blocks that are being transmitted between said first and second nodes.
2. The method of claim 1 wherein said first node is an optical line terminal (OLT) of a point-to-multipoint optical communications network and wherein said second node is one of multiple optical network units (ONUs) in said point-to-multipoint optical communications network.
3. The method of claim 2 further including a step of broadcasting said switch-to-new-key code to all of said multiple ONUs.
4. The method of claim 3 further including a step of switching to new keys at said ONUs in response to said broadcast of said switch-to-new-key code.
5. The method of claim 4 wherein said information blocks are formatted according to the IEEE 802.3 protocol.
6. The method of claim 5 wherein said step of signaling includes a step of utilizing an unused ten bit code in an eight bit to ten bit encoding scheme to generate said switch-to-new-key code.

7. The method of claim 6 wherein said step of signaling includes a step of replacing an idle code between two information blocks with said switch-to-new-key code.
- 5 8. The method of claim 1 wherein said step of signaling includes a step of generating an out-of-band signal as said switch-to-new-key code.
9. The method of claim 8 wherein said step of generating an out-of-band signal includes a step of utilizing an unused ten bit code in an eight bit to ten bit
10 encoding scheme to generate said switch-to-new-key code.
10. The method of claim 1 wherein said step of signaling includes a step of replacing an idle code between two information blocks with said switch-to-new-key code.

15

11. A method for maintaining synchronization between a key used by a source node to encrypt information within information blocks that are transmitted via a communications network to a destination node and a key used by said destination node to decrypt information within information blocks received from said source node, each information block including a header and a payload, said method comprising:

generating a new key at either said source node or said destination node; transmitting said new key from the node where said new key was generated to the other of said source and destination nodes;

generating a switch-to-new-key code that is not part of said header or said payload of any information blocks that are transmitted from said source node to said destination node;

transmitting said switch-to-new-key code from said source node to said destination node;

encrypting, with said new key, said payload of said information blocks that are transmitted from said source node after said switch-to-new-key code is transmitted; and

decrypting, with said new key, said payload of said information blocks that are received at said destination node after said switch-to-new-key code is received.

12. The method of claim 11 wherein said source node is an optical line terminal (OLT) of a point-to-multipoint optical communications network and wherein said destination node is one of multiple optical network units (ONUs) in said point-to-multipoint optical communications network.

13. The method of claim 12 further including a step of broadcasting said switch-to-new-key code to all of said multiple ONUs.

14. The method of claim 13 further including a step of switching to new keys at said ONUs in response to said broadcast of said switch-to-new-key code.

15. The method of claim 14 wherein said information blocks are formatted according to the IEEE 802.3 protocol.

5 16. The method of claim 15 wherein said step of generating a switch-to-new-key code includes a step of utilizing an unused ten bit code in an eight bit to ten bit encoding scheme to generate said switch-to-new-key code.

10 17. The method of claim 16 wherein said step of generating a switch-to-new-key code includes a step of replacing an idle code between two information blocks with said switch-to-new-key code.

15 18. The method of claim 11 wherein said step of generating a switch-to-new-key code includes a step of generating an out-of-band signal as said switch-to-new-key code.

19. The method of claim 18 wherein said step of generating an out-of-band signal includes a step of utilizing an unused ten bit code in an eight bit to ten bit encoding scheme to generate said switch-to-new-key code.

20 20. The method of claim 11 wherein said step of generating a switch-to-new-key code includes a step of replacing an idle code between two information blocks with said switch-to-new-key code.

21. A method for maintaining synchronization between keys used by an optical line terminal (OLT) to encrypt information within information blocks that are transmitted via a point-to-multipoint optical communications network to a plurality of optical network units (ONUs) and keys used by said plurality of ONUs to decrypt information within information blocks received from said OLT, each information block including a header and a payload, said method comprising:

generating new ONU-specific keys at said plurality of ONUs;

transmitting said new ONU-specific keys from said plurality of ONUs to

said OLT;

generating, at said OLT, a switch-to-new-key code that is not part of said header or said payload of any information blocks that are transmitted from said OLT to said plurality of ONUs;

transmitting said switch-to-new-key code from said OLT to said plurality of

ONUs;

encrypting, with said new ONU-specific keys, said payload of said information blocks that are transmitted from said OLT after said switch-to-new-key code is transmitted; and

decrypting, with said new ONU-specific keys, said payload of said information blocks that are received at said plurality of ONUs after said switch-to-new-key code is received.

22. The method of claim 21 wherein said switch-to-new-key code is received by each of said plurality of ONUs and wherein each of said ONUs switch to said new ONU-specific keys in response to said switch-to-new-key code.

23. The method of claim 21 wherein said switch-to-new-key code is an out-of-band signal.

24. The method of claim 21 wherein said switch-to-new-key code includes an unused ten bit code in an eight bit to ten bit encoding scheme.

25. The method of claim 24 wherein said information blocks are formatted according to the IEEE 802.3 protocol.

26. The method of claim 24 wherein said information blocks are transmitted
5 according to the 1000BASE-X specification of the IEEE 802.3 protocol.

27. The method of claim 21 further including:

transmitting upstream switch-to-new-key codes from said plurality of ONUs to said OLT;

10 encrypting, with a new upstream key, information blocks that are transmitted from said plurality of ONUs to said OLT after said upstream switch-to-new-key codes are transmitted; and

decrypting, with said new upstream key, said information blocks that are received at said OLT after said upstream switch-to-new-key code is received.

15

28. The method of claim 27 wherein said upstream switch-to-new-key code is transmitted from said plurality of ONUs in response to receiving said switch-to-new-key code from said OLT.

20 29. The method of claim 21 further including:

transmitting a use-broadcast-key code from said OLT to said plurality of ONUs;

encrypting, with a broadcast key, a specific number of information blocks after said use-broadcast-key code is transmitted; and

25 decrypting, with said broadcast key, said specific number of information blocks after said use-broadcast-key code is received.

30. A system for maintaining synchronization between a key used by a first node to encrypt information within information blocks that are transmitted via a communications network to a second node and a key used by said second node to decrypt information within information blocks received from said first node, each information block including a header and a payload, said system comprising:

means for distributing a new key between said first node and said second node; and

means for signaling, to one of said first and second nodes, a switch to said new key with a switch-to-new-key code that is not part of said header or said payload of any of said information blocks that are transmitted between said first and second nodes.

31. The system of claim 30 wherein said first node is an optical line terminal (OLT) of a point-to-multipoint optical communications network and wherein said second node is one of multiple optical network units (ONUs) in said point-to-multipoint optical communications network.

32. The system of claim 31 wherein said switch-to-new-key code is transmitted to all of said multiple ONUs simultaneously.

33. The system of claim 32 wherein said OLT includes a key synchronization unit for generating said switch-to-new-key code and wherein said ONUs include a key synchronization unit for identifying said switch-to-new-key code and for triggering a switch to said new key for decryption of said information after said switch-to-new-key code is identified.

34. The system of claim 31 wherein said OLT and said ONUs include packet controllers for generating information blocks that are formatted according to the IEEE 802.3 protocol.

35. The system of claim 30 wherein said switch-to-new-key code replaces an idle code that is located between two packets.

36. The system of claim 30 wherein said switch-to-new-key code includes an
5 unused ten bit code in an eight bit to ten bit encoding scheme.

37. A system for maintaining synchronization between keys used by an optical line terminal (OLT) to encrypt information within information blocks that are transmitted via a point-to-multipoint optical communications network to a plurality of optical network units (ONUs) and keys used by said plurality of ONUs to decrypt information within information blocks received from said OLT, each information block including a header and a payload, said system comprising:

said OLT; and

said plurality of ONUs;

said OLT including;

an OLT encryption controller for encrypting information within information blocks using ONU-specific keys;

a key synchronization unit for generating a switch-to-new-key code that is not part of said header or said payload of any information blocks that are transmitted from said OLT to said plurality of ONUs and for causing said OLT encryption controller to use new ONU-specific keys to encrypt information within information blocks that are transmitted after said switch-to-new-key code is transmitted to said plurality of ONUs;

each of said plurality of ONUs including:

a key generator for generating a new ONU-specific key that is transmitted to said OLT;

an ONU encryption controller for decrypting information within information blocks using an ONU-specific key;

a key synchronization unit for identifying said switch-to-new-key code that is transmitted from said OLT and for causing said ONU encryption controller to use said new ONU-specific key to decrypt information within said information blocks after said switch-to-new-key code is received from said OLT.

38. The system of claim 37 wherein said switch-to-new-key code is transmitted from said OLT to each of said ONUs simultaneously.

39. The system of claim 37 wherein each of said multiple ONUs switches to said
5 ONU-specific keys in response to the same switch-to-new-key code from said OLT.

40. The system of claim 37 wherein said OLT and said ONUs include packet
10 controllers for generating information blocks that are formatted according to the IEEE 802.3 protocol.

41. The system of claim 37 wherein said switch-to-new-key code replaces an idle code that is located between two packets.

42. The system of claim 37 wherein said switch-to-new-key code includes an
15 unused ten bit code in an eight bit to ten bit encoding scheme.